StoneGate 5.2

Common Criteria Certification User's Guide

StoneGate Firewall/VPN 5.2

SMC 5.2

STONESOFT

Secure Information Flow

Legal Information

End-User License Agreement

The use of the products described in these materials is subject to the then current end-user license agreement, which can be found at the Stonesoft website:
www.stonesoft.com/en/support/eula.html

Third Party Licenses

The StoneGate software includes several open source or third-party software packages. The appropriate software licensing information for those products at the Stonesoft website:
www.stonesoft.com/en/support/third_party_licenses.html

U.S. Government Acquisitions

If Licensee is acquiring the Software, including accompanying documentation on behalf of the U.S. Government, the following provisions apply. If the Software is supplied to the Department of Defense (“DoD”), the Software is subject to “Restricted Rights”, as that term is defined in the DOD Supplement to the Federal Acquisition Regulations (“DFAR”) in paragraph 252.227-7013(c) (1). If the Software is supplied to any unit or agency of the United States Government other than DOD, the Government’s rights in the Software will be as defined in paragraph 52.227-19(c) (2) of the Federal Acquisition Regulations (“FAR”). Use, duplication, reproduction or disclosure by the Government is subject to such restrictions or successor provisions.

Product Export Restrictions

The products described in this document are subject to export control under the laws of Finland and the European Council Regulation (EC) N:o 1334/2000 of 22 June 2000 setting up a Community regime for the control of exports of dual-use items and technology (as amended). Thus, the export of this Stonesoft software in any manner is restricted and requires a license by the relevant authorities.

General Terms and Conditions of Support and Maintenance Services

The support and maintenance services for the products described in these materials are provided pursuant to the general terms for support and maintenance services and the related service description, which can be found at the Stonesoft website:
www.stonesoft.com/en/support/view_support_offering/terms/

Replacement Service

The instructions for replacement service can be found at the Stonesoft website:
www.stonesoft.com/en/support/view_support_offering/return_material_authorization/

Hardware Warranty

The appliances described in these materials have a limited hardware warranty. The terms of the hardware warranty can be found at the Stonesoft website:
www.stonesoft.com/en/support/view_support_offering/warranty_service/

Trademarks and Patents

The products described in these materials are protected by one or more of the following European and US patents: European Patent Nos. 1065844, 1189410, 1231538, 1259028, 1271283, 1289183, 1289202, 1304849, 1313290, 1326393, 1379046, 1330095, 131711, 1317937 and 1443729 and US Patent Nos. 6,650,621; 6 856 621; 6,885,633; 6,912,200; 6,996,573; 7,099,284; 7,127,739; 7,130,266; 7,130,305; 7,146,421; 7,162,737; 7,234,166; 7,260,843; 7,280,540; 7,302,480; 7,386,525; 7,406,534; 7,461,401; 7,721,084; and 7,739,727 and may be protected by other EU, US, or other patents, or pending applications. Stonesoft, the Stonesoft logo and StoneGate, are all trademarks or registered trademarks of Stonesoft Corporation. All other trademarks or registered trademarks are property of their respective owners.

Disclaimer

Although every precaution has been taken to prepare these materials, THESE MATERIALS ARE PROVIDED "AS-IS" and Stonesoft makes no warranty to the correctness of information and assumes no responsibility for errors, omissions, or resulting damages from the use of the information contained herein. All IP addresses in these materials were chosen at random and are used for illustrative purposes only.

Revision: SGCC_20110930

Table of Contents

Chapter 1
Using StoneGate Documentation 5

Objectives and Audience 6
Product Documentation 7
Support Documentation 7
System Requirements 8
Supported Features 8
Contact Information 8

Chapter 2
Requirements for a Common Criteria Certified Installation 9

Certified Software 10
StoneGate Firewall Engine Software 10
Evaluated Hardware 10
Evaluated Network Topology 10
Configuration Specifics 11
About FIPS-compatible Operating Mode 11
Assumptions About the Intended Environment . 12
Secure Usage Assumptions 12
Administrator Access 12
Administrator Attributes 12
Environment Audit Procedures 12
Audit Support 12
Information Flow Control 12
Attack Level 13
General IT Environment Support 13
Self Protection Support 13
Shared Secret Key Management 13
User Authentication for Information Flow Control 13
Organizational Security Policies 13

Chapter 3
Installing StoneGate 15

Configuration Overview 16
Obtaining a Common Criteria Certified Product Version 16
Installing the Management Server and Log Server 17
Starting the Management Center 17
Defining a Single Firewall 18
Defining a Firewall Cluster 19
Modifying the Default Template for a Common Criteria Installation 20
Installing StoneGate Engines 21
Upgrading StoneGate Appliances to the Certified Engine Version 21
Configuring the Firewall Engine 21
Verifying Activation of FIPS-compatible Operating Mode 22
Resetting the Appliance to Factory Settings . . 22
Recovering from a FIPS 140-2 Self-test Failure . 23

Chapter 4
Implementing User Authentication 25

Configuring User Authentication 26

CHAPTER 1

USING STONEGATE DOCUMENTATION

Welcome to StoneGate™ High Availability Firewall and VPN solution from Stonesoft Corporation.

This chapter describes how to use the *Common Criteria Certification User's Guide* and related StoneGate documentation. It also provides directions for obtaining technical support and giving documentation feedback.

The following sections are included:

- Objectives and Audience (page 6)
- Contact Information (page 8)

Objectives and Audience

This *Common Criteria Certification User's Guide* provides information needed to implement a StoneGate solution according to Common Criteria (CC) evaluated guidelines. In addition, it provides supplemental user information that is not included in the regular Stonesoft, StoneGate product documentation. This guide is intended to be used in conjunction with the following StoneGate documentation when installing and configuring a CC certified StoneGate solution:

- The StoneGate Administrator's Guide.
- The StoneGate Management Center Installation Guide.
- The StoneGate Firewall/VPN Installation Guide.

This guide does not reproduce the above mentioned documentation. Rather, it simply supplements them by identifying specific configuration criteria that are required for a Common Criteria certified installation. Any configuration that falls outside of the evaluated configuration or security assumptions outlined in this guide should be considered an insecure state with respect to CC certification.

Typographical Conventions

The following conventions are used throughout the documentation:

Table 1.1 Typographical Conventions

Formatting	Informative Uses
User Interface text	Text you see in the User Interface (buttons, menus, etc.) and any other interaction with the user interface are in **bold-face**.
References, terms	Cross-references and first use of acronyms and terms are in *italics*.
`Command line`	File names, directories, and text displayed on the screen are `monospaced`.
`User input`	User input on screen is in **`monospaced bold-face`**.
`Command parameters`	Command parameter names are in *`monospaced italics`*.

We use the following ways to indicate important or additional information:

Note – Notes prevent commonly-made mistakes by pointing out important points.

Caution – Cautions prevent breaches of security, information loss, or system downtime. Cautions always contain critical information that you must observe.

Tip – Tips provide additional helpful information, such as alternative ways to complete steps.

Example Examples present a concrete scenario that clarifies the points made in the adjacent text.

Documentation Available

StoneGate technical documentation is divided into two main categories: Product Documentation and Support Documentation. StoneGate Firewall/VPN and StoneGate IPS have their separate sets of manuals, despite the fact that they are managed through the same user interface. Only the *Administrator's Guide* and the Online Help cover both the Firewall/VPN and IPS products.

Product Documentation

The table below lists the available guides. PDF versions of these guides are available on the Management Center CD-ROM and at http://www.stonesoft.com/support/.

Table 1.2 Product Documentation

Guide	Description
Reference Guide	Explains the operation and features of StoneGate comprehensively. Demonstrates the general workflow and provides example scenarios for each feature area. Available for StoneGate Firewall/VPN and StoneGate IPS.
Installation Guide	Instructions for planning, installing, and upgrading a StoneGate system. Available for StoneGate Management Center, StoneGate Firewall/VPN, and StoneGate IPS.
Online Help	Detailed instructions for configuration and use. Accessible through the Help menu and by using the Help button or the F1 key in any window or dialog. Available in the StoneGate Management Client and the StoneGate Monitoring Client. An HTML-based system is available in the StoneGate SSL VPN Administrator through help links and icons.
Administrator's Guide	Describes how to configure and manage the system step-by-step. Available as a combined guide for both StoneGate Firewall/VPN and StoneGate IPS, and as separate guides for StoneGate SSL VPN and StoneGate IPsec VPN Client.
User's Guide	Instructions for end-users. Available for the StoneGate IPsec VPN Client and the StoneGate Monitoring Client.
Appliance Installation Guide	Instructions for physically installing and maintaining StoneGate appliances (rack mounting, cabling etc.). Available for all StoneGate hardware appliances.

Support Documentation

The StoneGate support documentation provides additional and late-breaking technical information. These technical documents support the StoneGate Guide books, for example, by giving further examples on specific configuration scenarios.

The latest StoneGate technical documentation is available on the Stonesoft website at http://www.stonesoft.com/support/.

System Requirements

The system requirements for running StoneGate, including the approved network interfaces, supported operating systems, and other such hardware and software requirements for StoneGate engines and the Management Center can be found at http://www.stonesoft.com/en/products/fw/Software_Solutions/ (see the technical requirements section at the bottom of the page).

The hardware and software requirements for the version of StoneGate you are running can also be found in the *Release Notes* included on the Management Center CD-ROM and on the software download page at the Stonesoft website.

Supported Features

Not all StoneGate features are supported on all platforms. See the Appliance Software Support Table at the Stonesoft Support Documentation pages for more information.

Contact Information

For street addresses, phone numbers, and general information about StoneGate and Stonesoft Corporation, visit our website at http://www.stonesoft.com/.

Licensing Issues

You can view your current licenses at the License Center section of the Stonesoft website at https://my.stonesoft.com/managelicense.do.

For license-related queries, e-mail order@stonesoft.com.

Technical Support

Stonesoft offers global technical support services for Stonesoft's product families. For more information on technical support, visit the Support section at the Stonesoft website at http://www.stonesoft.com/support/.

Your Comments

We want to make our products suit your needs as best as possible. We are always pleased to receive any suggestions you may have for improvements.

- To comment on software and hardware products, e-mail feedback@stonesoft.com.
- To comment on the documentation, e-mail documentation@stonesoft.com.

Security Related Questions and Comments

You can send any questions or comments relating to StoneGate and network security to *security-alert@stonesoft.com*. A PGP key is available at http://www.stonesoft.com/en/support/support_contact_information/index.html.

Other Queries

For queries regarding other matters, e-mail info@stonesoft.com.

CHAPTER 2

REQUIREMENTS FOR A COMMON CRITERIA CERTIFIED INSTALLATION

This chapter outlines the specific software, hardware, and network configuration necessary for a certified installation.

The following sections are included:

- Certified Software (page 10)
- Evaluated Hardware (page 10)
- Evaluated Network Topology (page 10)
- Configuration Specifics (page 11)
- Secure Usage Assumptions (page 12)
- Assumptions About the Intended Environment (page 12)

Certified Software

Caution – It is highly recommended that you check your Stonesoft software prior to installation to ensure its integrity. The SHA1 checksum is available from the StoneGate product download page of Stonesoft's Website for this purpose at www.stonesoft.com. Also check all Known Issues and possible Security Advisories from Stonesoft's Website prior to installation.

StoneGate Firewall Engine Software

- The StoneGate Firewall Engine software application, version 5.2.5.8081.cc.2.
- The AuthenTec QuickSec IPsec Toolkit, version 5.1.

Evaluated Hardware

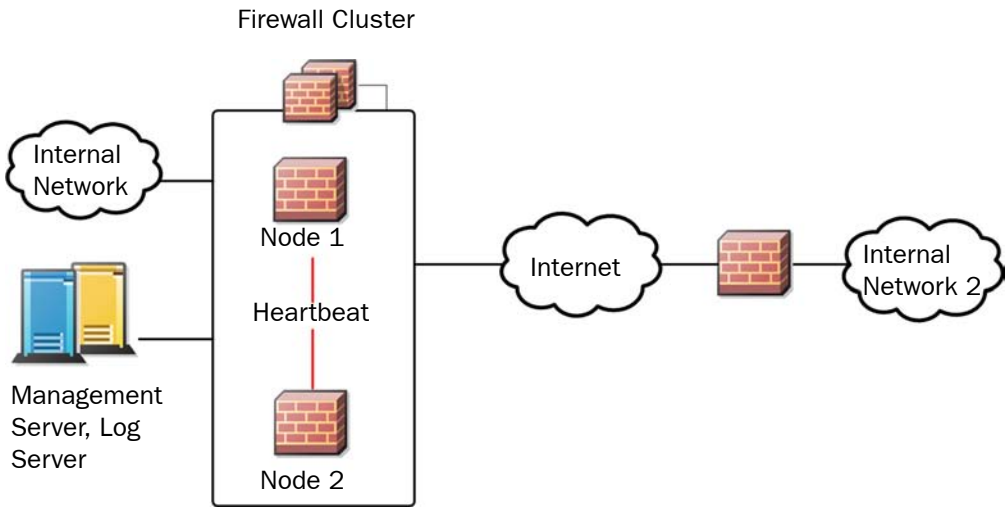
The following StoneGate models are included within the evaluation scope:

- FW-315
- FW-1301
- FW-3201
- FW-3205

Evaluated Network Topology

In its evaluated configuration, StoneGate is installed as a firewall cluster, with a VPN created between the cluster and a third StoneGate firewall. The exact network configuration required for certification is detailed in Illustration 2.1.

Illustration 2.1 Evaluated Network Configuration



Configuration Specifics

A CC certified installation also requires specific configurations as follows:

- Install the Management Server and Log Server on a trusted and separate management network.
- Use IPv4 addresses in configuring the firewall.
- Use a dedicated network for the Heartbeat between the nodes of the firewall cluster.
- Enable **FIPS-compatible operating mode** on the Advanced Settings tab of the Firewall properties and in the command line Engine Configuration Wizard.
- Set the Log Spooling Policy to **Stop Traffic** on the Advanced Settings tab of the Firewall properties.

Note – If the engine goes to the offline state due to the log spooling policy and it is manually forced back to the online state, the traffic flow through the node will continue. However, in this case no new log entries will be generated until there is enough disk space available.

About FIPS-compatible Operating Mode

By default, StoneGate supports some encryption algorithms that do not have FIPS approval. When FIPS-compatible operating mode is enabled, the following configuration changes are done automatically:

- access to the command line interface of the firewall engine is disabled
- the cryptographic module is configured to be in FIPS 140-2 mode
- VPN profile options that are not permitted in an FIPS-compatible configuration are disabled.

Specifically, FIPS-compatible operating mode disables the DES, Blowfish, Twofish and CAST-128 encryption algorithms, the AES-XCBC-MAC message authentication code, and the MD5 hash algorithm. FIPS-compatible operating mode allows RSA, DSA, Diffie-Hellman, 3DES, AES-128, AES-256 and SHA-1 algorithms for the use of the VPN. Furthermore, FIPS-compatible operating mode prohibits the use of plain AH as the IPsec Type. FIPS requires that if pre-shared secrets are used as the authentication method, the key size must be greater than or equal to 80 bits.

Additionally, RC4 and MD5 are disabled for communication between a Firewall node and the Management Server, Log Server and IPS components. CAST-128 and RIPEMD-160 are disabled for the heartbeat communication between the nodes of a Firewall cluster.

Because MD5 is used for passwords stored in StoneGate's internal LDAP user database, the internal LDAP user database cannot be used to store user passwords when FIPS-compatible operating mode is enabled.

Assumptions About the Intended Environment

This section identifies environmental assumptions that must exist in order to have a secure StoneGate installation. They include the following:

- Secure Usage Assumptions
- Organizational Security Policies

Secure Usage Assumptions

Administrator Access

During installation, Administrators can access the StoneGate engine via a command line interface to the firewall operating system or through the Management Server. After installation, the command line interface is disabled and Administrators can only access the StoneGate engine via the Management Server. The Management Server and StoneGate engine must be on a trusted and separate management network. In addition, administrators must have StoneGate configured so that identification and authentication is required to access both the operating system and the Management Server application.

Administrator Attributes

All authorized administrators must be trained, qualified, non-hostile individuals and must follow all instructions and guidance outlined in Stonesoft, StoneGate product documentation.

The administrator has the option of installing or reinstalling the engine in order to detect possible modifications to the StoneGate engine.

If the StoneGate engine is installed by a Value Added Reseller (VAR), the end-user must establish that the VAR fulfills the requirements for trusted administrator attributes as described above.

Environment Audit Procedures

Administrators must ensure that procedures exist to ensure that the audit trails are regularly analyzed and archived.

Audit Support

The IT environment generates audit records for the security functions on which the StoneGate engine depends from its environment. It also provides protected permanent storage of the audit trails generated by the StoneGate engine, including reliable timestamps for the audit records.

Information Flow Control

The IT environment of the engine must ensure that information can not flow among the internal and external networks unless it passes through the engine, and it must provide residual information protection for those packets. The IT environment of the engine must also provide secure storage of and access to the network security policy and user authentication data, and it must provide a reliable timestamp to support time-based information flow control decisions.

Attack Level

For CC certification purposes, the threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered moderate.

General IT Environment Support

The StoneGate firewall engines, the StoneGate Management Server and the management network must be dedicated to the firewall system. This means that they are not used for any other purpose other than operating StoneGate. In addition, administrators must ensure that all of the above are functioning according to their specifications, are physically secure, and that physical access is only allowed to trusted administrators.

Self Protection Support

The IT environment of the StoneGate engine must protect itself against attempts by unauthorized users to bypass, deactivate, or tamper with its security functions.

Shared Secret Key Management

The key used for Shared Secret SGW authentication must be generated and entered into the StoneGate engine in accordance with your organization's security policies and must follow all guidance information provided in StoneGate product documentation. The key size must be greater than or equal to 80 bits. The destruction of the key must be in accordance with the organization’s security policies and follow the guidance provided in StoneGate product documentation.

User Authentication for Information Flow Control

The IT environment must provide a user authentication mechanism for the StoneGate engine to use when the firewall policy requires users to authenticate before information can flow between the internal and external networks.

Organizational Security Policies

The StoneGate engine must use a cryptographic module for its cryptographic operations and associated key management that is compliant with FIPS PUB 140-2 (level 1).

CHAPTER 3

INSTALLING STONEGATE

This chapter explains how to install a Common Criteria certified StoneGate solution. Installation is done in accordance with the instructions provided in the *StoneGate Installation Guide*. When doing so, however, refer to this chapter for a detailed explanation of the specific engine and Management System configurations necessary for a certified installation.

The following sections are included:

- Configuration Overview (page 16)
- Obtaining a Common Criteria Certified Product Version (page 16)
- Installing the Management Server and Log Server (page 17)
- Starting the Management Center (page 17)
- Defining a Single Firewall (page 18)
- Defining a Firewall Cluster (page 19)
- Modifying the Default Template for a Common Criteria Installation (page 20)
- Installing StoneGate Engines (page 21)
- Recovering from a FIPS 140-2 Self-test Failure (page 23)

Configuration Overview

1. Obtain a Common Criteria certified product version (see Obtaining a Common Criteria Certified Product Version (page 16)).
2. Install the Management Server and Log Server (see Installing the Management Server and Log Server (page 17)).
3. Create Firewall elements in the Management Client and save the initial configuration (one-time password for Management Contact) for each firewall engine (see Defining a Firewall Cluster (page 19) and Defining a Single Firewall (page 18)).
4. Install the Common Criteria certified engine software version (see Installing StoneGate Engines (page 21)).

Obtaining a Common Criteria Certified Product Version

The process for ordering, obtaining, and installing a certified product version is as follows:

▼ To obtain a Common Criteria certified product version

1. Order a Common Criteria certified version from Stonesoft.
   - The plastic bag containing the appliance is sealed using security tape.
   - The appliance is delivered with the standard software version that is shipping at the time of the order and a Delivery Pack that includes the information to download StoneGate Common Criteria User's Guide.
   - Tracking information for the shipment is provided to you.
2. Track the shipment to make sure that the appliance is not lost, or the delivery delayed unnecessarily.
3. When the appliance arrives, verify that the appliance plastic bag and the security tape are intact.
4. Download the Common Criteria certified software from Stonesoft's website at www.stonesoft.com.
5. Contact Stonesoft Support by e-mail or phone and verify the SHA-1 checksum. If e-mail is used, the Stonesoft Support PGP private key is used to sign the e-mail reply message. Verify the signature using the Stonesoft Support PGP public key available at Stonesoft's website at http://www.stonesoft.com/en/support/support_contact_information/index.html.

Begin the installation by Installing the Management Server and Log Server (page 17).

Installing the Management Server and Log Server

This section outlines the specific configuration parameters for the Management Server and Log Server. This section is meant to be used in conjunction with the *StoneGate Installation Guide* when installing and configuring the Management Server and Log Server.

▼ To install the Management Server and Log Server

1. Start the installation as instructed in the **Getting Started with Management Center Installation** section of the *StoneGate Management Center Installation Guide*.
2. Select the appropriate installation options for your environment as instructed in the **Installing Management Center Components** section of the *StoneGate Management Center Installation Guide*.
3. Configure the Management Server properties for your environment as instructed in the **Installing a Management Server** section of the *StoneGate Management Center Installation Guide*.
4. Configure the Log Server properties for your environment as instructed in the **Installing a Log Server** section of the *StoneGate Management Center Installation Guide*.
5. Finish the installation as instructed in the **Finishing the Installation** section of the *StoneGate Management Center Installation Guide*.

Continue by Starting the Management Center.

Starting the Management Center

When starting the Management Center for the first time, the following steps must be completed:

▼ To start the Management Client

1. Start the Management Server as instructed in the **Starting the Management Server** section of the *StoneGate Management Center Installation Guide*.
2. Log in using the Management Client as instructed in the **Logging in to the Management Center** section of the *StoneGate Management Center Installation Guide*.
3. Install license files using the Management Client as instructed in the **Installing Licenses** section of the *StoneGate Management Center Installation Guide*.
4. Start the Log Server as instructed the **Starting the Log Server and Web Portal Server** section of the *StoneGate Management Center Installation Guide*.

Continue to the next relevant section:

- To define a single firewall, proceed to Defining a Single Firewall (page 18).
- To define a firewall cluster, proceed to Defining a Firewall Cluster (page 19).

Defining a Single Firewall

This section outlines the specific configuration parameters for the Single Firewall configuration procedure that prepares the Management Center for a StoneGate firewall installation. It is meant to be used in conjunction with the *StoneGate Administrator's Guide*. The single firewall is configured in the Management Client.

▼ To define a single firewall

1. Define Single Firewall elements as instructed in the **Adding a Single Firewall Element** section of the *StoneGate Firewall/VPN Installation Guide*.
2. Define physical interfaces as instructed in the **Adding Physical Interfaces** section of the *StoneGate Firewall/VPN Installation Guide*.
3. (*Optional*) Define VLAN interfaces as instructed in the **Adding VLANs** section of the *StoneGate Firewall/VPN Installation Guide*.
4. Define IP Addresses as instructed in the **Configuring IP Addresses for Physical, VLAN, or ADSL Interfaces** section of the *StoneGate Firewall/VPN Installation Guide*.

Note – Use only IPv4 addresses. IPv6 addresses are not supported with all features.

5. Set interface options as instructed in the **Settings Global Interface Options** section of the *StoneGate Firewall/VPN Installation Guide*.
6. Switch to the **Advanced** tab of the Firewall Properties and configure the following options:
   - Select **FIPS-compatible operating mode**.

Caution – Selecting this option only disables configuration options that are not available in FIPS-compatible operating mode in the Management Client. It does not enable FIPS-compatible operating mode on the engine. You must enable FIPS-compatible operating mode during the initial configuration of the appliance.

   - Click **Log Handling** and set the Log Spooling Policy to **Stop Traffic** in the dialog that opens.
7. Click **OK** in the Firewall Properties dialog. The Firewall element is created.
8. Bind management-bound licenses to specific firewall elements as instructed in the **Binding Engine Licenses to Correct Elements** section of the *StoneGate Firewall/VPN Installation Guide*.
9. Save the defined configuration for use during Firewall installation as instructed in the **Saving the Initial Configuration for Firewall Engines** section of the *StoneGate Firewall/VPN Installation Guide*.

Caution – Handle the configuration files securely. They include the one-time password that allows establishing trust with the Management Server.

Continue to the next relevant section:

- If you are also installing a firewall cluster, proceed to Defining a Firewall Cluster (page 19).
- Otherwise, proceed to Modifying the Default Template for a Common Criteria Installation (page 20).

Defining a Firewall Cluster

This section outlines the specific configuration parameters for the Firewall Cluster configuration procedure that prepares the Management Center for a StoneGate firewall installation. It is meant to be used in conjunction with the *StoneGate Installation Guide*. The firewall cluster is configured in the Management Client.

▼ To define a firewall cluster

1. Define Firewall Cluster elements as instructed in the of the **Adding a Firewall Cluster Element** section of the *StoneGate Firewall/VPN Installation Guide*.
2. (*Optional*) Add nodes to the Firewall Cluster as instructed in the **Adding Nodes to a Firewall Cluster** section of the *StoneGate Firewall/VPN Installation Guide*.
3. Define physical interfaces as instructed in the **Adding Physical Interfaces** section of the *StoneGate Firewall/VPN Installation Guide*.
4. (*Optional*) Define VLAN interfaces as instructed the **Adding VLANs** section of the *StoneGate Firewall/VPN Installation Guide*.
5. Define CVIs and NDIs as instructed in the **Defining Contact Addresse for Firewall Clusters** section of the *StoneGate Firewall/VPN Installation Guide*.
6. Set interface options as instructed in the **Setting Global Interface Options for Clusters** section of the *StoneGate Firewall/VPN Installation Guide*.
   - **Packet Dispatch** is the recommended CVI mode. Other CVI modes can be used if necessary.
   - Use a dedicated network for the Heartbeat between the nodes of the firewall cluster. In addition to the mandatory **Primary** Heartbeat Interface, we recommend configuring a **Backup** Heartbeat Interface.
7. Switch to the **Advanced** tab of the Firewall Properties and configure the following options:
   - Select **FIPS-compatible operating mode**.

Caution – Selecting this option only disables configuration options that are not available in FIPS-compatible operating mode in the Management Client. It does not enable FIPS-compatible operating mode on the engine. You must enable FIPS-compatible operating mode during the initial configuration of the appliance.

   - Click **Log Handling** and set the Log Spooling Policy to **Stop Traffic** in the dialog that opens.
8. Click **Clustering**. The Clustering Properties dialog opens.
9. Verify in the Node Synchronization section that **Sync Security Level** is **Sign** or **Encrypt and Sign**.
   - If necessary, change the Sync Security as instructed in the **Adjusting Firewall Clustering Options** section of the *StoneGate Administrator's Guide*.
   - When the Sync Security Level is Sign, all synchronization messages are authenticated using a keyed-hash message authentication code and all sensitive messages are also encrypted. The exchange of the key is encrypted and authenticated using digital signatures. This level of security prevents outside injections of connection state information. It is the default security level.
   - When the Sync Security Level is Encrypt and Sign, all messages are both encrypted and authenticated. This level of security increases the overhead compared to the Sign option, but is strongly recommended if the node-to-node are relayed through insecure networks.
10. Click **OK** in the Firewall Properties dialog. The Firewall Cluster element is created.

11. Bind management-bound licenses to specific firewall elements as instructed in the **Binding Engine Licenses to Correct Elements** section of the *StoneGate Firewall/VPN Installation Guide*.

12. Save the defined configuration for use during Firewall installation as instructed in the **Saving the Initial Configuration for Firewall Engines** section of the *StoneGate Firewall/VPN Installation Guide*.

Caution – Handle the configuration files securely. They include the one-time password that allows establishing trust with the Management Server.

Continue by Modifying the Default Template for a Common Criteria Installation.

Modifying the Default Template for a Common Criteria Installation

The Default Firewall Policy template must be modified to block Services that are not compatible with a Common Criteria installation.

▼ To modify the Default Template for a Common Criteria installation

1. Select **Configuration→Configuration→Firewall**. The Firewall Configuration view opens.
2. Right-click the Default template policy and select **Edit Firewall Template Policy**. The template policy opens for editing.
3. Locate the IPV4 Access rule that has the following properties:

Table 3.1 SG VPN Client Configuration Rule

ID	Source	Destination	Service	Action
5	ANY	$$Local cluster (CVI Addresses Only)	SG Blacklisting SG User Authentication SG VPN Client Configuration	Allow

4. Right-click **SG VPN Client Configuration** in the Service cell and select **Remove SG VPN Client Configuration**.
5. Right-click **SG Blacklisting** in the Service cell and select **Remove SG Blacklisting**.
6. Right-click the ID cell of the modified rule and select **Add Rule Before** to add a rule with the following properties:

Table 3.2 New SG VPN Client Configuration Rule

ID	Source	Destination	Service	Action
	ANY	$$Local cluster	SG VPN Client Configuration	Discard

7. Select **File → Save As** and save this new template under a unique name.

Whenever you create security policies that will be used in FIPS mode, use this newly created template as the template for the new security policies.

Continue by Installing StoneGate Engines (page 21).

Installing StoneGate Engines

In a Common Criteria certified installation, the StoneGate engine must be a StoneGate firewall appliance. In a clustered configuration, each node in the firewall cluster must be configured individually. Begin the engine configuration on the appliance by Upgrading StoneGate Appliances to the Certified Engine Version.

Upgrading StoneGate Appliances to the Certified Engine Version

StoneGate appliances are delivered with the most recent engine software preinstalled. The engine software must be upgraded to the certified engine version before entering FIPS-compatible operating mode. This is necessary even if the same version was installed previously, because the file system checksum is stored during the upgrade process.

▼ To upgrade to the certified engine version

1. Save the Common Criteria certified engine upgrade zip file in the root directory of a USB memory stick or obtain a Common Criteria certified engine upgrade zip file on CD-ROM from Stonesoft support.

Note – The engine upgrade zip file must be in the root directory of the media.

2. Contact Stonesoft support using the PGP key available at http://www.stonesoft.com/en/support/support_contact_information/index.html to obtain the correct SHA1 checksum.
3. Boot up the appliance. The Engine Configuration Wizard starts.
4. Select **Upgrade**. The Select Source Media dialog opens.
5. Select **USB Memory** or **CD-ROM**. The upgrade starts.
6. Select **OK**. The engine reboots and the Engine Configuration Wizard starts with the Engine image verification dialog shown. Select **Calculate SHA1**. The SHA1 checksum is calculated and displayed below the checksum from the engine image zip file.
7. Verify that the calculated checksum is identical to the checksum from the zip file and that both checksums match the checksum provided by Stonesoft Support. Select **OK**.
8. Select **OK**. The engine reboots.
9. Check the Engine version to make sure that the certified version is loaded.

Continue as instructed in Configuring the Firewall Engine (page 21).

Configuring the Firewall Engine

▼ To configure the firewall engine

1. Start the Engine Configuration Wizard as instructed in the **Configuring the Engine in the Engine Configuration Wizard** section of the *StoneGate Firewall/VPN Installation Guide*.
2. Configure the Operating System settings as instructed in the **Configuring the Operating System Settings** section of the *StoneGate Firewall/VPN Installation Guide*.
   - Select **Restricted FIPS-compatible operating mode**. The SSH daemon and root password options are automatically disabled in the Engine Configuration Wizard.

3. Configure the network interfaces according to your environment as instructed in the **Configuring the Network Interfaces** section of the *StoneGate Firewall/VPN Installation Guide*.
4. Contact the Management Server as instructed in the **Contacting the Management Server** section of the *StoneGate Firewall/VPN Installation Guide*.
   - **Enter node IP address manually** is selected by default and other IP Address options are disabled when FIPS-compatible operating mode is enabled.

The engine restarts. Continue by Verifying Activation of FIPS-compatible Operating Mode.

Verifying Activation of FIPS-compatible Operating Mode

Restricted FIPS-compatible operating mode must be enabled during the initial configuration of the appliance. The following steps describe how to verify that FIPS-compatible operating mode has been activated.

▼ To verify activation of FIPS-compatible operating mode

1. Verify that the following messages are displayed on the console when the engine restarts:
   - `FIPS: rootfs SHA1 integrity check OK`
     (displayed after the root file system integrity test has been executed successfully)
   - `FIPS power-up tests succeeded`
     (displayed after the FIPS 140-2 power-up tests have been executed successfully)
2. Open the Logs view in the Management Client and verify that the following message is shown in the logs:
   - Started in FIPS 140-2 operating mode.
3. Continue as instructed in the **After Successful Management Server Contact** section of the *StoneGate Firewall/VPN Installation Guide*.

Note – If the engine does not enter FIPS-compatible operating mode even though it is configured to do so ("Started in non-FIPS 140-2 approved operating mode" is shown in the logs), or if the power-up tests fail (a power-up test error message is displayed or the success message is not displayed), the appliance must be reset to factory settings and reinstalled as instructed in Recovering from a FIPS 140-2 Self-test Failure.

Resetting the Appliance to Factory Settings

Resetting the appliance to factory settings is not part of the normal installation procedure. There is no need to reset the appliance to factory settings before starting to use it for the first time. These instructions can be used to reset the appliance to factory settings when necessary, such as when initial configuration has been completed without enabling the Restricted FIPS-compatible operating mode, during use, or when the appliance is being removed from use.

▼ To reset the appliance to factory settings

1. Reboot the appliance and select **System restore options** from the boot menu. StoneGate Engine System Restore starts.
2. Enter **2** for **Advanced data removal options**.
3. Enter one of the following options:
   - **1** for **1 pass overwrite**.
   - **8** for a **Custom** number of overwrite passes.

4. If you selected **Custom**, enter the number of overwrite passes. A larger number of overwrites is more secure, but it may take a considerable amount of time depending on the appliance storage capacity.

Recovering from a FIPS 140-2 Self-test Failure

If the FIPS 140-2 power-up self-tests fail, or the engine does not enter FIPS-compatible operating mode, the appliance must be reset to factory settings and reinstalled according to these instructions. Begin by Resetting the Appliance to Factory Settings.

▼ To recover from a FIPS 140-2 self-test failure

1. Reset the appliance to factory settings as instructed in Resetting the Appliance to Factory Settings (page 22).
2. Repeat the engine version upgrade as instructed in Upgrading StoneGate Appliances to the Certified Engine Version (page 21).
3. Configure the firewall engine and enable FIPS-compatible operating mode as instructed in Configuring the Firewall Engine (page 21).
4. Verify that FIPS-compatible operating mode is activated as instructed in Verifying Activation of FIPS-compatible Operating Mode (page 22).

CHAPTER 4

IMPLEMENTING USER AUTHENTICATION

This chapter explains how to configure user authentication.

The following sections are included:

- Configuring User Authentication (page 26)

Configuring User Authentication

Because MD5 is used for passwords stored in StoneGate's internal LDAP user database, the internal LDAP user database cannot be used to store user passwords when FIPS-compatible operating mode is enabled. Authentication based on username and password requires an external LDAP server, which you can optionally integrate with StoneGate to create different rules for each user. An External RADIUS or TACACS+ Authentication Server can be used for password authentication to the firewall.

This section outlines the specific configuration parameters for user authentication. It is meant to be used in conjunction with the *StoneGate Administrator's Guide*.

▼ To configure user authentication

1. (*For external user database only*) Configure LDAP integration. For instructions, see the **Integrating External LDAP Databases** section of the *StoneGate Administrator's Guide*.
2. (*For external authentication server only*) Create the Authentication Server and Authentication Service elements to integrate the external authentication server in your StoneGate-enforced authentication scheme. For detailed instructions, see the **Defining an Authentication Server** and **Defining an Authentication Service** sections of the *StoneGate Administrator's Guide*.
   - Create a **RADIUS Authentication Server** or **TACACS+ Authentication Server**.
   - Select **RADIUS** or **TACACS+** as the **Type** for the Authentication Service.
3. Define the User Group and User information. For instructions, see the **Defining User Accounts for Authentication** section of the *StoneGate Administrator's Guide*.
4. Create and install Access rules with authentication defined. For instructions, see the **Defining Authentication Rules** section of the *StoneGate Administrator's Guide*.
5. (*Optional*) Customize the authentication prompt that end-users see when they authenticate using a Telnet client. For instructions, see the **Customizing the User Authentication Dialog** section of the *StoneGate Administrator's Guide*.

StoneGate Guides

Administrator's Guides - step-by-step instructions for configuring and managing the system.

Installation Guides - step-by-step instructions for installing and upgrading the system.

Reference Guides - system and feature descriptions with overviews to configuration tasks.

User's Guides - step-by-step instructions for end-users.

For more documentation, visit
www.stonesoft.com/support/

Stonesoft Corporation

Itälahdenkatu 22 A
FI-00210 Helsinki
Finland

Tel. +358 9 476 711
Fax +358 9 4767 1349

STONESOFT

Secure Information Flow

Stonesoft Inc.

1050 Crown Pointe Parkway
Suite 900
Atlanta, GA 30338
USA

Tel. +1 770 668 1125
Fax +1 770 668 1131